ARMY RESEARCH LABORATORY

A Policy-Driven Information Exchange Network

by Mark R. Mittrick, John T. Richardson, and Richard C. Kaste

ARL-MR-704 **July 2008**

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Aberdeen Proving Ground, MD 21005-5067

ARL-MR-704 **July 2008**

A Policy-Driven Information Exchange Network

Mark R. Mittrick, John T. Richardson, and Richard C. Kaste
Computational and Information Sciences Directorate, ARL

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED (From - To)
July 2008	Final	October 2006–May 2008

4. TITLE AND SUBTITLE
A Policy-Driven Information Exchange Network

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mark R. Mittrick, John T. Richardson, and Richard C. Kaste

5d. PROJECT NUMBER
W911NF-05-2-0039

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRD-ARL-CI-IC
Aberdeen Proving Ground, MD 21005-5067

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-MR-704

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Tactical information exchange, involving levels of interdependent and sometimes conflicting policies, presents many difficulties. This is a critical problem for today's fighting forces, one that the U.S. Army Research Laboratory's Brigade and Below Battlespace Awareness Network project is addressing.
In certain battlefield situations, mechanisms must be implemented to allow information to move across domains. A major objective of the project is to develop decision-making capabilities for releasing information, using KAoS, which was developed at the Institute for Human and Machine Cognition. KAoS policy services allow for the specification, management, conflict resolution, and enforcement of policies within domains. In an attempt to remedy the cross-domain issue, these services test policies that incorporate tactical awareness into the information release decision.
Innovative solutions require changes in information policy as well as new models and methods. Requirements for and impediments to tactical information exchange, integration with academic/industrial software, simulated data sets for experimentation, and techniques for implementing a prototype are investigated. This report provides an overview of our research in support of a policy-driven information exchange network.

15. SUBJECT TERMS
B3AN, policy information exchange, KAoS redaction

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mark Mittrick
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL	24	19b. TELEPHONE NUMBER (*Include area code*) 410-278-4148

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Contents

List of Figures

Acknowledgments

This report would not have been possible without the outstanding efforts of Eric Heilman, Larry Bunch, and Jeff Bradshaw. Mr. Heilman was instrumental in developing the scenario and associated data products. Mr. Bunch was the KAoS technical lead and provided much auxiliary programmatic support. Dr. Bradshaw interfaced with the California State University San Bernardino Policy Working Group and offered valuable suggestions. This work was performed under the auspices of two U.S. Army Research Laboratory Collaborative Agreements (W911NF-05-2-0039, Foundation for CSU San Bernardino; W911NF-07-2-0088, Policy Governed Data Fusion).

INTENTIONALLY LEFT BLANK.

1. Introduction

The goal of the U.S. Army Research Laboratory's (ARL's) Brigade and Below Battlespace Awareness Network (B3AN) project is the realization of a tactical information exchange system drawing upon various intelligence sources available to the military. An important aspect of the project is the handling of heterogeneous data types and sources. For example, data could include unmanned aerial vehicle imagery or a "spot report" in audio or text format. Furthermore, rapid exchange of available information is essential for success in urban conflicts. Accurate and timely intelligence is critical to maintaining the situational awareness needed for battlefield dominance. Despite the need for rapid exchange, it is critical for any solution to account for existing policies governing access to these data types and sources in order to remain consistent with security protocols. The technical challenge of B3AN is designing an automated information exchange system while attempting to maintain security requirements.

One product from this effort is a software system to demonstrate the utility of a policy engine. Developing and testing such software entails pursuing and applying of scholarly research with our academic partners concerning requirements for and impediments to cross-domain information exchange, prototypical components through extensions to semantic filtering/transformations, and possible integration with academic/industrial software.

The work here is qualitatively different from and complementary to other related efforts pursued at ARL. This was a new beginning; because a sensitive area and somewhat controversial approaches are involved, the technical and programmatic aspects are complicated. This work does not intend to short-circuit existing security policy procedures or guard development and implementation mechanisms; rather, the tactical application is considered a research thrust.

2. Challenges

A formulation of the overall problem might be how a "classified" data item can be transformed for release to a "lesser-cleared" user to maximize the value of perishable information. The hypothesis is that bringing "classified" information, with policy issue resolution, to a lesser-classified level is a powerful enabler of situation understanding. A more general problem would involve maximizing the value of released information relative to arbitrary security criteria.

The system needs to define "need to know," which can take a variety of forms and include temporal, geographic, or organizational aspects. A temporal aspect to need to know could be based on relevance of the information to the user. The Soldier needs to know what is around the corner—the information is relevant to the Soldier only at that moment. To an analyst in the

chain of command, the information could be more relevant with regard to battle damage assessment or predictive course of action development. Those involved in training might also use the information for a very long time after the event.

When a unit is performing a mission, it is bounded by an area of operations (AO), or area of responsibility, to ensure mission execution without interfering with another unit. Geographic qualification would include the Soldier's relation to the event being viewed. The relationship could be defined by proximity or by the fact that the Soldier and event are in the same AO.

Similarly, the notion of chain of command must be considered as a factor in tactical information access by the Soldier. The system must address the need to know of the chain and associated analysts. That is, for most U.S. Army situations, the Soldier's actions are ordered or coordinated by other personnel involved with the mission. These people must generally be permitted to monitor inputs to the operator. Need to know is also complicated by the existence of combat support and combat service support entities. For example, artillery may not be in the direct chain of command but could be involved in aspects of the specific battlespace, requiring intelligence concerning portions of the execution. This could be associated not only with positive support but also with mishap avoidance.

One component of the research involves rationales for requiring certain pieces of information. This leads to philosophical considerations that combine tactical aspects of the scenario and larger implications of transformation and dissemination. For instance, if one knew he or she were walking into an ambush, a certain sensing would help. If the system has such information, should it be passed along in any event? What if passing it along might cause greater damage than the benefit? One could argue that a central clearinghouse is needed; in some schemes, the human security officer fills this role. It often appears that many real-world problems do not lend themselves to automatic policy processing and that amenable situations are contrived and simplistic. This situation can at least be partially addressed by today's information technology. A hybrid approach that utilizes emerging semantic web technology seems appropriate in the fast-paced complex battlespace.

The notion of situational imperative is essential to policy development for tactical information release. This entails assessing the necessity of information to the recipient as well as of associated urgency. (Note that necessity and urgency may be related but are separate concepts.) A fact may be necessary to avoid a tactical error, in general, but it is not urgent. An example might be the size of the enemy force in the next sector. Similarly, the notion of information perishability is required. In general, assessing value of information is a significant research problem; assessing time- or event-dependent value, required for tactical policy solutions, is even more complicated.

The total policy system should take into account time intervals and scheduling with regard to transformation, release, and use of information. Another related complication involves the notions of partial mission completion and partial information release. It is tempting to think of a "complete" fact or sensing as impacting an "entire" mission. However, there is a spectrum of mission completion, in terms of goals accomplished and progress toward accomplishment. The developers and users of policy systems must take into account that information may be released piecemeal to subsets of the agents working a mission. The reason information may be released piecemeal is that the calculations of situational imperative will likely assign varying prioritizations.

3. Scenario

One of the goals here is to construct a demonstration that will help convince policy makers of the need to change current information-sharing methods. In this demonstration, an event (e.g., a new threat report) will precipitate a proper mission response and illustrate how emerging technology might ameliorate situations in which existing policy/procedures would have interfered with situational awareness and mission execution. The following is the sequence from this effort:

- The 3rd brigade combat team (BCT) is on a peace-keeping mission in central and southern Diyala.
- Delta Company (part of 3rd BCT) is located in southern Diyala.
- Alpha Company (part of 3rd BCT) is located in northern Diyala.
- Alpha Company collects human intelligence (HUMINT) report concerning an incendiary explosive device (IED) factory in a small town.
- The IED factory may relocate at anytime, so the HUMINT is perishable.
- The division orders 3rd BCT to investigate the IED factory.
- The 3rd BCT creates a fragmentary order (FRAGO) for Delta Company to perform cordon and search on the village.
- B3AN helps determine the intelligence package that Delta Company gets for its mission.
- Delta Company destroys the IED factory and captures high-profile terrorists and documents.

For visualization, existing McKenna military operations in urban terrain (MOUT) site backgrounds and tactical overlays were used (figure 1).

Figure 1. McKenna (Fort Benning, GA) MOUT.

4. Policies

The policies that the team derived for the scenario are listed next and can be found in more detail in the paper "Policy-Governed Information Exchange in a U.S. Army Operational Scenario."[1]

4.1 Authorization Policies

- Brigade Combat Team (BCT) members are authorized to access documents that have a classification level of secret or below (e.g., secret, sensitive, and unclassified).
- Company members are authorized to access documents that have a classification level of secret and are perishable.
- Company members are authorized to access documents that have a classification level of sensitive or below.

4.2 Approval Policies

- BCT members are obligated to approve Company member access to documents that are sensitive or above.

[1] Institute of Human and Machine Cognition. Policy-Governed Information Exchange in a U.S. Army Operational Scenario. *The 2008 IEEE Workshop on Policies for Distributed Systems and Networks*, Palisades, NY, June 2008.

- Except: BCT members are not obligated to approve company member access to HTML documents that are sensitive and perishable.

4.3 Redaction Policies

- BCT members are obligated to redact source-identifying text for Company member accesses to HTML documents that are sensitive or above.

4.4 Notification Policies

- BCT members are obligated to notify the creator of any orders containing priority INTEL requirements that match the features of a received document.

5. Policy Aware Information Exchange

ARL, in collaboration with the Institute for Human Machine Cognition (IHMC), developed a demonstration system to test an automated policy-based solution to tactical information exchange inside the bounds of the scenario. The system uses IHMC's KAoS policy services framework to determine the intelligence information available for a mission. KAoS employs the Web Ontology Language (OWL) to represent and reason about the policies defining access to intelligence documents. The system requires an XHTML representation of the intelligence documents to enable the embedding of ontology information in the form of resource description framework (RDF) attribute markup. Finally, the system uses Simple Protocol and RDF Query Language (SPARQL), a language that can perform queries on OWL, to identify documents relevant to the mission and filter the results based on policies represented in KAoS.

To illustrate the process of matching appropriate intelligence documents to a mission, consider the situation displayed in figure 2. This figure represents the point in the scenario when the 3rd BCT has issued a FRAGO to Delta Company. The BCT intelligence analyst has loaded an XHTML version of the FRAGO into the demonstration client, enabling the system to parse the mission type (AttackMission) and AO (village T-12). The SPARQL query coded into the system will identify intelligence documents relevant to an attack mission in the given AO. The ontology defines relevant information for attack missions (figure 3).

It is evident why the system identified the document highlighted in figure 2 (0831 SITREP) as relevant. The RDF meta-data embedded in this report (figure 4) reveals that the document includes information in the target AO (village T-12). Furthermore, the report represents an enemy threat (no. a_EnemyThreat in the meta-data), which matches a type of relevant information for an AttackMission displayed in figure 3 (no. a_Threat).

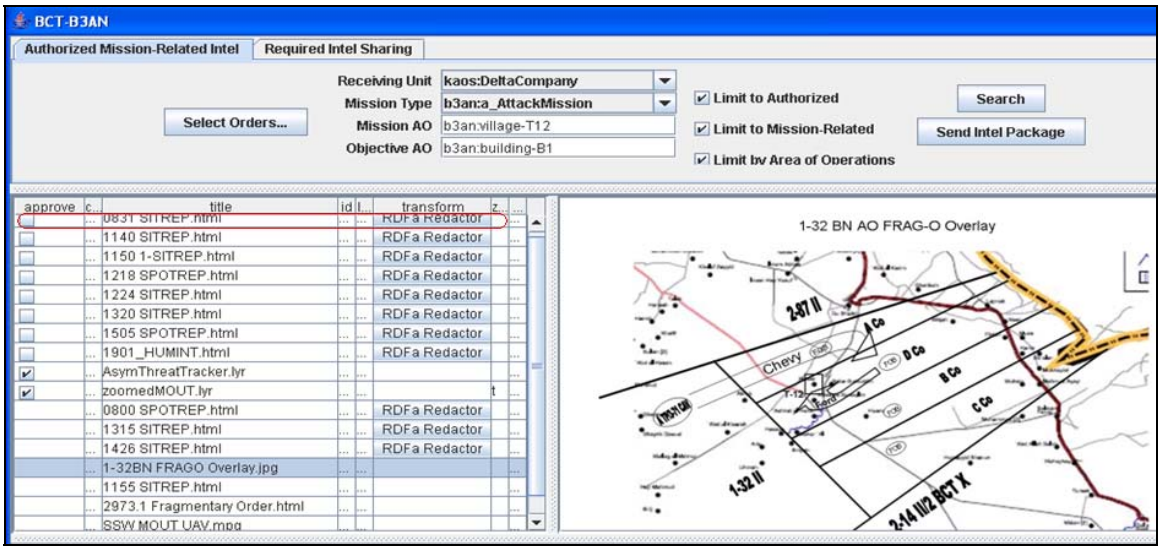

Figure 2. BCT client.

```
<AttackMission rdf:ID="a_AttackMission">
   <p-missionPriorityInfo rdf:resource="#a_Alert"/>
   <p-missionPriorityInfo rdf:resource="#a_Threat"/>
```

Figure 3. AttackMission ontology snippet.

```
<div property="http://www.w3.org/1999/02/22-rdf-syntax-ns#type"
      content="http://localhost/b3an/meta/b3an-intel-ontology.owl#SITREP"/>
<div property="http://localhost/b3an/meta/b3an-intel-ontology.owl#title"
      content="0831 SITREP"/>
<div property="http://localhost/b3an/meta/b3an-intel-ontology.owl#identifier"
      content="http://localhost/b3an/data/0831%20SITREP.html"/>
<div property="http://localhost/b3an/meta/b3an-intel-ontology.owl#classification-level"
      content="http://localhost/b3an/meta/b3an-intel-ontology.owl#a_Secret"/>
<div property="http://localhost/b3an/meta/b3an-intel-ontology.owl#perishability"
      content="http://localhost/b3an/meta/b3an-intel-ontology.owl#a_Perishable"/>
<div property="http://localhost/b3an/meta/b3an-intel-ontology.owl#p-geoScope"
      content="http://localhost/b3an/meta/b3an-intel-ontology.owl#village-T12"/>
<div property="http://localhost/b3an/meta/b3an-intel-ontology.owl#p-feature"
      content="http://localhost/b3an/meta/b3an-intel-ontology.owl#a_EnemyThreat"/>
```

Figure 4. SITREP meta-data.

Next, the SPARQL query filters the identified documents against the authorization policies to determine release eligibility. The authorization policies defined in KAoS state that the BCT is allowed to access the document (0831 SITREP) because its embedded meta-data defines it as secret and perishable (figure 4). Furthermore, the policies obligate the BCT commander to approve or disapprove the release of the report to Delta Company. According to policy, if a document represents information above sensitive classification, then commander approval is required before releasing it for mission use. This security control is in the BCT client (figure 2) as a check box next to the document. Finally, if the document is used for the mission, then any statements identifying the source (i.e., informant name) of the intelligence must be redacted. This condition stems from another policy concerning documents classified above sensitive.

Redaction is possible because the intelligence documents are written in XHTML. This format allowed ARL developers to use an extensible markup language (XML) parser to find and remove elements containing source-revealing information by searching for relevant RDF attribute markup. For example, in figure 5, the highlighted code includes RDF attribute markup identifying the text 'P-3' identifying the source of the imagery. In the mission version of this document, the text 'P-3' will not be included. The source code for the redaction methods is available in the appendix.

```
<div>
 <h3>0831 SITREP</h3>
</div>
<div>
 <table>
  <tr><td id="label">From:</td>
      <td id="val">1-327<sup>th</sup> BN</td></tr>
  <tr><td id="label">To:</td>
      <td id="val">2/A/1-327 BN</td></tr>
  <tr><td id="label">Line Alpha:</td>
       <td id="val">No change in threat situation.</td></tr>
  <tr><td id="label">Line Bravo:</td>
       <td id="val">Friendly forces remain on latest orders.  New
      <span property="http://localhost/b3an/meta/b3an-intel-ontology.owl#contributor">P-3</span>
      imagery available within the hour.</td></tr>
  <tr><td id="label">Line Echo:</td>
      <td id="val">VX chemical weapon threat credible in vicinity village Smith.  Go to MOP level 1.</td></tr>
 </table>
</div>
```

Figure 5. Redaction meta-data.

6. Possible Research

Our initial investigations have precipitated several research possibilities. As the software implementations of the foundational policy work are developed, approaches to and implications of related problems are considered. Working on these will lead to improvements in the B3AN

model and better approaches to tactical policy semantics. These vary considerably, and overlap somewhat, but can be grouped roughly into a few categories.

One category deals with fundamental issues of information in general. For instance, can appropriate mathematics dealing with measurement or calculation of the value of information be developed? How about the mathematics of risk? The problem involves several preliminary semantic, almost philosophical aspects. Certain "parameters" must first be defined before ways to determine or measure their values can be discussed.

Another category is explicitly tactical and applied. Here, techniques for measuring or calculating perishability, urgency of mission, and proximity in space/time/mission are considered. These things may require subject matter expert consultation, particularly with regard to partial mission completion. Tactical classification is not (totally) ordered; it is more akin to "need to know." Perhaps the following new "security categories" other than (U) and (S) should be recognized: types (A) and (B), depending on the situational parameters discussed. Is it possible for any item to be transformed? If not, what are the policy repercussions? Is it possible for this whole process to be completely automated by computers such as the fictional SkyNet? Can there be notions of the "inherent" classification of composite/transformed data?

How can cost (in terms of time, fidelity, and robustness) of the process, particularly with a human in the loop, be properly accounted for?

A kind of hybrid category between theoretical and applied involves questions listed next. How can a security policy model handle recipient knowledge of the existence of data fields? How about assessing the ability of an entity to deduce unauthorized information? These things are related to the practical notion of constraining types of queries in order to mitigate unintended disclosure. What are the implications of partial release (e.g., can release these parts to these entities), even if explicit deduction does not apply?

Continuing with hybrid aspects, it is difficult to evaluate the downside of inappropriate release. For instance, although information may be vital to mission completion, there is a finite chance that it may fall into the hands of the enemy. Items and subitems entering into policy applications are typically not independent. Many interrelated and even essentially unquantifiable aspects could make it an impossible problem, or these aspects could seem so situation-dependent that human decision makers must be involved.

A thesis to prove or disprove the further research just outlined would extend the basic hypothesis as set forth in this report. This extended hypothesis, which can be dealt with analytically, can be stated as follows: situational imperative and information perishability is necessary but not sufficient.

7. Conclusion

A policy-driven information exchange network would ideally have many benefits, including secure automation of configuration, quality of service, and other aspects of network management. It is hoped that groundbreaking work on rule-based access control by IHMC will lead to improvements in extensibility, verifiability, and efficiency. Planning for longer term extensions includes studying scholarly research; aligning tasks with this research; integrating with academic/industrial software; enabling web services aspects (e.g., agents); refining rules; and developing a robust object-based B3AN policy model.

INTENTIONALLY LEFT BLANK.

Appendix. Redaction Code

This appendix appears in its original form, without editorial change.

APPENDIX

Redaction Code

```
package b3an.redact;

import java.io.ByteArrayOutputStream;
import java.io.InputStream;
import java.io.OutputStream;
import java.util.Vector;

import org.apache.xerces.parsers.DOMParser;
import org.w3c.dom.DOMImplementation;
import org.w3c.dom.Document;
import org.w3c.dom.Node;
import org.w3c.dom.bootstrap.DOMImplementationRegistry;
import org.w3c.dom.ls.DOMImplementationLS;
import org.w3c.dom.ls.LSOutput;
import org.w3c.dom.ls.LSSerializer;
import org.w3c.dom.traversal.DocumentTraversal;
import org.w3c.dom.traversal.NodeFilter;
import org.w3c.dom.traversal.NodeIterator;
import org.xml.sax.InputSource;

public class B3AN_Redact implements TextTransform {

    public B3AN_Redact() {
    }

    public String transform(Vector<String> strings, InputStream in)
            throws Exception {

        DOMParser p = new DOMParser();
        p.parse(new InputSource(in));
        Document d = p.getDocument();

        DocumentTraversal traversal = (DocumentTraversal) d;
        NodeIterator nIterator = traversal.createNodeIterator(d
                .getDocumentElement(), NodeFilter.SHOW_ALL, null, true);

        Node n = nIterator.getRoot();

        while (n != null) {
            boolean remove = false;

            if (n.hasAttributes()) {
                for (int i = 0; i < n.getAttributes().getLength(); i++) {
                    for (int j = 0; j < strings.size(); j++)
                        if (n.getAttributes().item(i).getTextContent()
                                .compareTo(strings.elementAt(j)) == 0)
                            remove = true;
                }
            }
            for (int j = 0; j < strings.size(); j++)
                if (n.getTextContent().compareTo(strings.elementAt(j)) == 0) {
                    remove = true;

                }
            if (remove)
                n.getParentNode().removeChild(n);

            n = nIterator.nextNode();
        }
```

```
        System.setProperty(DOMImplementationRegistry.PROPERTY,
                "org.apache.xerces.dom.DOMImplementationSourceImpl");
        DOMImplementationRegistry registry = DOMImplementationRegistry
                .newInstance();
        DOMImplementation domImpl = registry.getDOMImplementation("LS 3.0");
        DOMImplementationLS implLS = (DOMImplementationLS) domImpl;
        LSSerializer dom3Writer = implLS.createLSSerializer();
        LSOutput output = implLS.createLSOutput();
        OutputStream outputStream = new ByteArrayOutputStream();
        output.setByteStream(outputStream);
        output.setEncoding("UTF-8");
        dom3Writer.write(d, output);

        return outputStream.toString();
    }
}
```

INTENTIONALLY LEFT BLANK.

NO. OF COPIES	ORGANIZATION
1 (PDF ONLY)	DEFENSE TECHNICAL INFORMATION CTR DTIC OCA 8725 JOHN J KINGMAN RD STE 0944 FORT BELVOIR VA 22060-6218
1	US ARMY RSRCH DEV & ENGRG CMD SYSTEMS OF SYSTEMS INTEGRATION AMSRD SS T 6000 6TH ST STE 100 FORT BELVOIR VA 22060-5608
1	DIRECTOR US ARMY RESEARCH LAB IMNE ALC IMS 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB AMSRD ARL CI OK TL 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB AMSRD ARL CI OK T 2800 POWDER MILL RD ADELPHI MD 20783-1197

ABERDEEN PROVING GROUND

1	DIR USARL AMSRD ARL CI OK TP (BLDG 4600)

NO. OF
COPIES ORGANIZATION

1 DIR USARL
AMSRD ARL CI I
B BROOM
2800 POWDER MILL RD
ADELPHI MD 20783-1197

2 DIR USARL
AMSRD ARL CI IB
R WINKLER
L TOKARCIK
2800 POWDER MILL RD
ADELPHI MD 20783-1197

1 DIR USARL
AMSRD ARL CI NT
G CIRINCIONE
2800 POWDER MILL RD
ADELPHI MD 20783-1197

ABERDEEN PROVING GROUND

18 DIR USARL
AMSRD ARL CI IC
T HANRATTY
M MITTRICK (15 CPS)
J RICHARDSON
M THOMAS